JOURNAL OF ALGEBRA 34, 309–330 (1975)

# Counting Abelian Subgroups of p-groups. A Projective Approach

MARC KONVISSER AND DAVID JONAH

*Department of Mathematics, Wayne State University, Detroit, Michigan 48202*

*Communicated by B. Huppert*

Received September 13, 1973

We use the projective geometry of the maximal subgroups of a $p$-group to count (via P. Hall's Enumeration Theorem) the number of elements in certain classes $\mathscr{C}$ of abelian subgroups of a $p$-group $G$, $p \neq 2$. We look along the lines of this projective geometry to localize the counting to asking structural questions about the products of elements of $\mathscr{C}$ which are normal in $G$. We ask, when does each maximal subgroup of the product of two (and, sometimes, three) normal elements of $\mathscr{C}$ also contain an element of $\mathscr{C}$. We often answer this question by showing the existence of abelian subgroups of a specified order in a certain family of class 2 $p$-groups.

In the crucial case—counting elementary abelian subgroups of order $p^5$—we show that the number of such subgroups of a specific kind of group is the number of projective solutions to a homogeneous equation of degree 2 (quadratic form) in 3 variables. We get this quadratic form by using the cross product and dot product on a suitable 3-dimensional vector space over the field with $p$ elements.

We count, modulo $p$, the number of elements in three types of classes of abelian subgroups of a $p$-group $G$: the elementary abelian subgroups of a fixed order $p^k$, $k \leqslant 5$; the abelian subgroups of order $p^k$, for a fixed $k \leqslant 5$; and the abelian subgroups of a fixed index $p$ or $p^2$.

We use the results and techniques of the elementary abelian case to get the results in the abelian case. The abelian case is then used to get the index results. These are contained in the following theorem and its corollary.

THEOREM. *Let $G$ be a $p$-group, $p \neq 2$, and let $\mathscr{C}$ be any one of the following classes of abelian subgroups of $G$:*

(i) *elementary abelian subgroups of order $p^k$ for some fixed $k \leqslant 5$;*

(ii) *abelian subgroups of order $p^k$ for some fixed $k \leqslant 5$;*

(iii) *abelian subgroups of fixed index $p$ or $p^2$.*

*Suppose $\mathscr{C}$ is nonempty.*

*Then the number of elements of $\mathscr{C}$ (in $G$) is congruent to* 1 *modulo* $p$ *except in the index* $p^2$ *case where the number can also be exactly* 2.

COROLLARY. (i) *If $G$ is a normal subgroup of a $p$-group $\mathscr{X}$, then there are elements of $\mathscr{C}$ which are normal in $\mathscr{X}$.*

(ii) *If a $p$-group $\mathscr{X}$, $p \neq 2$, has an abelian subgroup of index $p^3$, then there is a normal abelian subgroup of index $p^3$ in $\mathscr{X}$.*

This theorem generalizes results of Berkovic [2, Theorem 1] for $p^3$ and [3, Theorem 11] for $p^4$. The corollary generalizes results of Huppert [13, III 7.5] for $p^2$; Feit–Thompson [5, Lemma 8.4] for $p^3$; Hobby [12, Theorem 1] for $p^4$; Alperin [1, Theorem 4] for index $p^2$ and $p^3$; and Konvisser [16, Theorems A, B] for $p^k$, $k \leqslant 5$, and index $p^2$, $p^3$.

We have several families of examples of $p$-groups with exactly 2 elementary abelian subgroups of order $p^6$ [14]; Berkovic [3] gives an example of a $p$-group with exactly $5p$ elementary abelian subgroups of order $p^7$. Berkovic uses this example to construct a group $G$ of order $5^{11}$ with exactly 25 abelian subgroups of order $5^7$ (index $5^4$) with all of them nonnormal in $G$.

The transition from the theorem (counting) to the corollary (normality) comes from the simple observation that when a $p$-group operates on a finite set then the nontrivial orbits have length a multiple of $p$. We formalize this as the following proposition which will be used repeatedly throughout the paper.

PROPOSITION 0.1. *Let $\mathscr{C}$ be a nonempty class of subgroups of a $p$-group $G$, let $\mathscr{C}$ be closed under conjugation, and for each subgroup $H$ of $G$ let $n(H)$ be the number of elements of $\mathscr{C}$ which are subgroups of $H$.*

*Then*

(i) *the number of elements of $\mathscr{C}$ which are not normal in $G$ is divisible by $p$.*

(ii) *$n(G)$ is congruent modulo $p$ to the number of elements of $\mathscr{C}$ which are normal in $G$.*

(iii) *if $n(G)$ is not divisible by $p$, then some element of $\mathscr{C}$ is normal in $G$.*

(iv) *if $N$ is a normal subgroup of $G$ with $n(N)$ not divisible by $p$, then $N$ contains an element of $\mathscr{C}$ which is normal in $G$.*

(v) *if $N$ is a normal subgroup of $G$ containing all of the elements of $\mathscr{C}$ which are normal in $G$, then $n(G) \equiv n(N) \bmod p$.*

*Notation* 0.2. We will often use the symbol $E_{p^k}$ to denote an elementary abelian $p$-group of rank $k$.

## 1. Line Lemma

In this section we set up machinery for counting, modulo $p$, certain types of abelian subgroups of $p$-groups, $p \neq 2$; in particular, elementary abelian and abelian subgroups of a fixed order $p^k$ for $k \leqslant 5$ and abelian subgroups of index $p$ or $p^2$.

The major tool for counting in $p$-groups is P. Hall's Enumeration Theorem [9, p. 39]. We use the following special case.

THEOREM 1.1. [P. Hall]. *Let $\mathscr{C}$ be a class of proper subgroups of a $p$-group $G$; for each subgroup $H$ of $G$, let $n(H)$ be the number of elements of $\mathscr{C}$ which are contained in $H$.*

*Then*

$$n(G) \equiv \sum_{M \max \text{ in } G} n(M) \bmod p.$$

We want to show that $n(G) \equiv 1 \bmod p$ given that for each maximal subgroup $M$: either $n(M) = 0$ or $n(M) \equiv 1 \bmod p$. In other words, given a fixed maximal subgroup $M_0$ with $n(M_0) \neq 0$ we want to show that the number of maximal subgroups $M \neq M_0$ with $n(M) \neq 0$ is a multiple of $p$ or equivalently, the number with $n(M) = 0$ is a multiple of $p$. This suggests that we use an equivalence relation on the set of maximal subgroups $M \neq M_0$ having $p$ elements in each equivalence class. Such a natural equivalence relation is available once we realize that the maximal subgroups $M$ of a $p$-group $G$ form a projective space with $p + 1$ points per line.

DEFINITION 1.2. The line $\overline{M_1 M_2}$ determined by two distinct maximal subgroups $M_1, M_2$ is the set of all maximal subgroups $M$ with $M \geqslant M_1 \cap M_2$.

PROPOSITION 1.3. *Let $\pi$ be a finite projective space in which each line contains $p + 1$ points and let $f$ be a function from the points of $\pi$ to the integers. Suppose there is a point $m_0$ of $\pi$ with the following property:*

*If $m_1$ and $m_2$ are two points different from $m_0$ on the same line through $m_0$, then $f(m_1) \equiv f(m_2) \bmod p$.*

*Then*

$$\sum_{m \in \pi} f(m) \equiv f(m_0) \bmod p.$$

*Proof.*

$$\sum_{m \in \pi} f(m) = f(m_0) + \sum_{\mathscr{L} \in \pi} \left( \sum_{m \in L'} f(m) \right),$$

where $\mathscr{L}$ is the pencil of all lines $L$ of $\pi$ containing the point $m_0$ and $L'$ is the set $L - \{m_0\}$. Furthermore,

$$\sum_{m \in L'} f(m) \equiv 0 \bmod p,$$

since $f$ is constant, by assumption, on the points of $L'$, a set with $p$ elements.

Applying these ideas to $p$-groups we get the following theorem.

LINE LEMMA 1.4. *Let $G$ be a $p$-group, let $\mathscr{C}$ be a class of proper subgroups of $G$, and let $n(H)$ be the number of elements of $\mathscr{C}$ contained in a subgroup $H$ of $G$. Suppose that:*

(i) *for each maximal subgroup $M$ which contains an element of $\mathscr{C}$, then $n(M) \equiv 1 \bmod p$.*

(ii) *there is a maximal subgroup $M_0$ with the property if a maximal subgroup $M_1 \neq M_0$ contains an element of $\mathscr{C}$, then so do all maximal subgroups $M$ on the line $\overline{M_0 M_1}$.*

*Then, if $\mathscr{C}$ is nonempty,*

$$n(G) \equiv 1 \bmod p.$$

*Proof.* Proposition 1.3 and Hall's Enumeration Theorem 1.1.

In order to maintain the focus on the geometry we give the following definitions.

DEFINITIONS 1.5. Let $\mathscr{C}$ be a class of subgroups of $p$-group $G$.

(i) A maximal subgroup $M_0$ which satisfies condition (ii) of the Line Lemma 1.4 is called an *origin* (for $\mathscr{C}$).

(ii) A proper subgroup $\mathscr{L}$ is called a *local origin* if for each maximal subgroup $M$ of $G$, the intersection $\mathscr{L} \cap M$ contains an element of $\mathscr{C}$.

(iii) A pair $E_1, E_2$ of elements of $\mathscr{C}$ is said to *support good lines* if each maximal subgroup $M \geqslant E_1 \cap E_2$ also contains an element of $\mathscr{C}$.

Besides meeting the inductive requirement (i) of the Line Lemma 1.4 we need ways to find origins. The normality requirements appear in the following because of our desire to localize the problem.

METHODS OF LOCATING ORIGINS 1.6. *Let $\mathscr{C}$ be a class, closed under conjugation, of proper subgroups of a $p$-group $G$ satisfying $n(M) = 0$ or $n(M) \equiv 1$ for each maximal subgroup $M$ (condition* (i) *of the Line Lemma).*

*Then $G$ contains an origin $M_0$ if any one of the following three conditions is satisfied.*

(i) *$G$ contains a local origin $\mathscr{L}$; in which case any maximal $M_0 \geqslant \mathscr{L}$ is an origin.*

(ii) *Each pair $E_1, E_2$ of elements of $\mathscr{C}$ which are normal in $G$ support good lines; in which case any maximal subgroup $M_0$ containing an element of $\mathscr{C}$ is an origin.*

(iii) *A maximal subgroup $M_0$ of $G$ contains a family $E_1, \ldots, E_m$ of normal elements of $\mathscr{C}$ satisfying: if $E$ is a normal element of $\mathscr{C}$, then for some $i$, $1 \leqslant i \leqslant m$, the pair $E, E_i$ supports good lines; in which case $M_0$ is an origin.*

*Proof.* (i) follows from the definitions.

(ii) Let $M_0$ be a maximal subgroup containing an element of $\mathscr{C}$. Then $M_0$ contains an element $E_0$ of $\mathscr{C}$ which is normal in $G$, since the conditions of (0.1 iv) are satisfied: $M_0$ is normal in $G$, $n(M_0) \equiv 1 \bmod p$, and $\mathscr{C}$ is closed under conjugation. For the same reasons each maximal subgroup $M_1$ contains a normal element $E_1$ of $\mathscr{C}$ whenever $M_1$ contains any element of $\mathscr{C}$. Thus each $M$ on the line $\overline{M_0 M_1}$ contains an element of $\mathscr{C}$, for $M \geqslant M_0 \cap M_1 \geqslant E_0 \cap E_1$ which in turn implies that $M$ contains an element of $\mathscr{C}$ because the normal pair $E_0, E_1$ supports good lines.

(iii) follows as in (ii).

The following simple application of these methods will illustrate how we use the Line Lemma to count, modulo $p$, subgroups of $p$-groups; specifically, how we use information about the product of two normal elements of $\mathscr{C}$ to count in $G$.

APPLICATION 1.7. *Let $G$ be a $p$-group, $p \neq 2$, containing an elementary abelian subgroup of order $p^2$.*

*Then the number of such subgroups is congruent to* 1 mod $p$.

*Furthermore,* [13, III 7.5] *any normal subgroup $N$ of $G$ containing an elementary abelian subgroup of order $p^2$ contains one which is normal in $G$.*

*Proof.* We may assume, by induction, that the counting result has been verified for all groups of orler less than $|G|$, in particular for the maximal subgroups $M$ of $G$. Let $G$ contain an elementary abelian subgroup of order $p^2$ and let $\mathscr{C}$ be the class of all such subgroups. By using proposition (0.1 iv) we see that $G$ contains at least one normal elementary abelian subgroup $E_1$ of order $p^2$. If there were no other normal one then $n(G) \equiv 1 \bmod p$ by (0.1 ii).

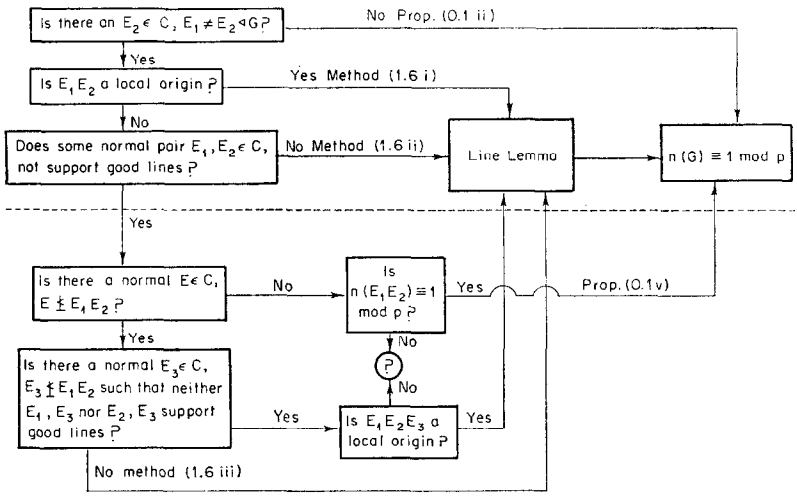
If $E_2 \neq E_1$ is a normal element of $\mathscr{C}$, then the product $E_1 E_2$ is a local origin as it is either elementary abelian of order $p^3$ or $p^4$ or it is the nonabelian group of order $p^3$ and exponent $p$. In each case, every maximal subgroup of $E_1 E_2$ contains an element of $\mathscr{C}$. (For the same reason the pair $E_1, E_2$ supports good lines.) Thus the Line Lemma gives the counting result.

To obtain Huppert's result from this we use (0.1 v).

In general the procedures for applying Methods (1.6 i, ii, iii) and the Line Lemma 1.4 are considerably more complicated. The following Flow Chart gives the decision procedures used in counting (elementary) abelian subgroups of order $p^k$, for some fixed $k \leqslant 5$. We will refer to this Flow Chart in our proofs of Theorems 2.2, 4.1, and 5.5.

FLOW CHART 1.8. *How the Line Lemma is used.*

Let $\mathscr{C}$, $G$, and $n(H)$ be as in 1.6. Assume further that $\mathscr{C}$ is nonempty so that by (0.1 iv) there is an $E_1 \in \mathscr{C}$ which is normal in $G$.




## 2. THE NUMBER OF ELEMENTARY ABELIAN SUBGROUPS OF RANK 4

In this section we count, modulo $p$, the number of elementary abelian subgroups of order $p^k$, $k \leqslant 4$ and $p \neq 2$. Specifically, we use Alperin's Theorem [1, Theorem 3] on two alternating forms to show that for any normal pair $E_1$, $E_2$ of such subgroups either the product $E_1E_2$ is a local origin or the pair $E_1$, $E_2$ supports good lines for the class of all elementary abelian subgroups of order $p^k$. In terms of the Flow Chart 1.8 we never have to cross the dotted line.

THEOREM 2.1. *Let $H = E_1E_2$ be the product of two normal elementary abelian subgroups $E_1 \neq E_2$ of order $p^k$, $p \neq 2$, such that either*

$$|H'| \leqslant p^2 \quad \text{or} \quad |H: Z(H)| \leqslant p^2.$$

*Then either $H$ contains an elementary abelian subgroup of order $p^{k+1}$ or else each maximal subgroup of $H$ containing $E_1 \cap E_2$ contains an elementary abelian subgroup of order $p^k$.*

*The first conclusion implies that the product $E_1E_2$ is a local origin and both say that the pair $E_1$, $E_2$ supports good lines for the class $\mathscr{C}$ of all elementary abelian subgroups of order $p^k$ of any $p$-group $G$ containing both $E_1$ and $E_2$.*

*Proof.* Since $E_1$ and $E_2$ are normal in $H$ and $p \neq 2$, we see that $H$ has class at most 2, has exponent $p$, and $Z(H) \geqslant E_1 \cap E_2$.

If $Z(H) > E_1 \cap E_2$, then either $E_1Z(H)$ or $E_2Z(H)$ is abelian of order at least $p^{k+1}$ and we are done. So in the remainder of the proof we take $Z(H) = E_1 \cap E_2$.

If $|H: Z(H)| = p^2$, then $|H| = p^{k+1}$ and every maximal subgroup $L$ of $H$ which contains $Z(H)$ is of order $p$ over $Z(H)$ and so is abelian, as desired.

So we are left to consider the case where $Z(H) = E_1 \cap E_2$ and $|H'| \leqslant p^2$. Let $|E_1 \cap E_2| = p^c$ so that $|H| = p^{2k-c}$. Now we will show that each maximal subgroup $L$ of $H$ containing $E_1 \cap E_2 = Z(H)$ also contains an elementary abelian subgroup of order $p^k$. To do this we apply a theorem of Alperin [1, Theorem 3] on pairs of alternating forms.

We obtain the forms as Alperin does—specifically: The subgroup $L$ has class at most 2 and $L' \leqslant Z(H) \leqslant Z(L)$. Let $N = Z(H)$. If $L$ is abelian there is no problem, so we look at the case where $|L'| = p$ or $p^2$. Let $L' = \langle c, d \rangle$ where $d = 1$ if $|L'| = p$, and define the alternating forms

$$f, g: L/N \times L/N \to GF(p)$$

by

$$[\bar{x}, \bar{y}] = c^{f(\bar{x},\bar{y})}d^{g(\bar{x},\bar{y})} \in L',$$

where $\bar{x}, \bar{y}$ denote the cosets $xN$, $yN$, respectively; we take $g = 0$ if $d = 1$.

Now Alperin's Theorem states that both $f$ and $g$ vanish on a common subspace of dimension at least $[(n + 1)/2]$, where $n$ is the dimension of the vector space $L/N$; i.e., $n = 2(k - c) - 1$. Hence $L$ contains an elementary abelian subgroup of dimension at least $(k - c) +$ (dimension of $Z(H)$) $= k$, as needed to complete the proof.

From this theorem we easily obtain the following which contains results of Berkovic, Hobby, Huppert, Feit–Thompson, and Konvisser. For specifics see the introduction.

THEOREM 2.2. *Let $G$ be a finite $p$-group, $p \neq 2$, containing an elementary abelian subgroup of order $p^k$ for some $k \leqslant 4$.*

*Then the number of elementary abelian subgroups of $G$ of order $p^k$ ($k \leqslant 4$) is congruent to 1 modulo $p$.*

*Furthermore, if a normal subgroup $N$ of $G$ contains an elementary abelian subgroup of order $p^k$ ($k \leqslant 4$), then $N$ contains one which is normal in $G$.*

*Proof.* We may assume by induction, that the counting result has been verified for all groups of order less than $|G|$, in particular for the maximal subgroups $M$ of $G$. Let $\mathscr{C}$ be the class of all elementary abelian subgroups of $G$ of order $p^k$ for some fixed $k \leqslant 4$.

Following the Flow Chart 1.8 it suffices (as in 1.7) to show that either the product $E_1E_2$ of two normal elements of $\mathscr{C}$ is a local origin or that each normal pair supports good lines. As we are working in this range $|E_1| = |E_2| \leqslant p^4$, the commutator group $[E_1, E_2]$ has order $\leqslant p^2$, meaning that Theorem 2.1 applies and we can use the Line Lemma. This gives the count modulo $p$.

The normality statement then follows from (0.1 iv).

In a similar fashion one proves the following:

THEOREM 2.3. *Let $G$ be a $p$-group, $p \neq 2$, with $G'$ elementary abelian of order dividing $p^2$. Suppose $G$ contains an elementary abelian subgroup of order $p^k$. Then the number of elementary abelian subgroups of $G$ of order $p^k$ is congruent to one modulo $p$.*

*Remark* 2.4. This result 2.3 is best possible in the sense that there are $p$-groups $G$, $p \neq 2$, with $G'$ elementary abelian of order $p^3$ which contain exactly two abelian subgroups of (maximal) order $p^k$ (cf. [14, Corollary 3.4, Example 4.6, and Chap. 6]).

## 3. $E_{p^5}$'s AND PROJECTIVE GEOMETRY

The count, modulo $p$, of elementary abelian subgroups of order $p^k$, $p \neq 2$ works for $k \leqslant 4$ because the product of two such normal $E_{p^k}$'s yields enough information to use the Line Lemma 1.4; specifically their commutator subgroup has small order ($\leqslant p^2$) or their product has a center of small index ($\leqslant p^2$) (cf 2.2). Thus for $k = 5$ we must also look at the product of two normal $E_{p^5}$'s whose commutator subgroup has order $p^3$. Such a group has order $p^7$ and exponent $p$.

In this section we will investigate a slightly more general class of groups; namely groups $G$ of order $p^7$ and exponent $p$ with $G' = Z(G)$ of order $p^3$. We show that each such group contains an $E_{p^5}$ and the number of $E_{p^5}$'s is $1, 1 + p, 1 + 2p$, or $1 + p + p^2$. Because of their unusual connections with projective geometry we take the time to classify them. There are just five isomorphism classes, each corresponding to a projective subvariety of the projective plane—point, line, double line, conic, and plane. The number of points on each subvariety is equal to the number of $E_{p^5}$'s. This connection is made precise by using the group $G$ to define a quadratic form $q$ and by showing that there is a one-to-one correspondence between the set of projective solutions to $q(v) = 0$ and the set of $E_{p^5}$'s of $G$.

The reader interested in just the counting results need only read through Theorem 3.2. The existence part of this theorem was obtained in [11, Satz 3] by highly computational methods.

A. *Translation from Commutation to Cross Product*

Let $G$ be a group of order $p^7$, exponent $p$, with $G' = Z(G)$ of order $p^3$. In addition, let $G$ have a maximal subgroup $A$ which does not have an $E_{p^5}$.

Under such circumstances, commutation

$$\begin{aligned}[\ ,\ ]: A/Z(G) \times A/Z(G) &\to G' \\ (xZ, yZ) &\to [x, y]\end{aligned}$$

is an alternating bilinear mapping on the three dimensional (multiplicative) vector space $A/Z(G)$.

We want to relate this alternating mapping to the cross product on a 3-dimensional (additive) vector space $V$ over the field $\mathrm{GF}(p)$, in order to make use of the standard interrelationships between the cross product, perpendicularity, and the dot product.

Recall that when $V$ is a vector space with basis $i, j, k$ the cross product is the alternating mapping $\times: V \times V \to V$ satisfying $i \times j = k$, $j \times k = i$, and $k \times i = j$, while the associated dot product is the symmetric bilinear form $\cdot: V \times V \to GF(p)$ satisfying $i \cdot i = j \cdot j = k \cdot k = 1$ and $i \cdot j = i \cdot k = j \cdot k = 0$. We will use the fact that:

3.1. If $v \neq 0$, then a vector $z$ of $V$ can be written as $z = v \times w$ for some $w \in V$ if and only if $z$ is perpendicular to $v$ which is true if and only if $v \cdot z = 0$.

We go from commutation to the cross product on a three dimensional (additive) vector space $V$ as follows. Let $\bar{a}_1$, $\bar{a}_2$, $\bar{a}_3$ be a basis of $A/Z(G)$ considered as a vector space over $GF(p)$; because $A$, by assumption, does not contain an $E_{p^5}$ and because $G' = Z(G)$ has order $p^3$, it follows that $[a_2, a_3]$, $[a_3, a_1]$, $[a_1, a_2]$ form a basis of $G'$. Thus there are isomorphisms $\phi: A/Z(G) \to V$, $\gamma: G' \to V$ such that the following diagram is commutative:

$$\begin{array}{ccccc} A/Z(G) & \times & A/Z(G) & \xrightarrow{[\ ,\ ]} & G' \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \gamma} \\ V & \times & V & \xrightarrow{\times} & V \end{array} \tag{1}$$

B. *The quadratic form*

With the above setup relating to any maximal subgroup $A$ which does not have an $E_{p^5}$, we can associate a quadratic form $q$ on $V$ as follows. For each

fixed element $u$ of $G$ not in such a maximal subgroup $A$, there is a linear mapping $T_u : V \to V$ corresponding to the linear mapping $aZ(G) \to [u, a]$ from $A/Z(G)$ to $G'$; specifically

$$\begin{array}{ccc} A/Z(G) & \xrightarrow{[u,\ ]} & G' \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \gamma} \\ V & \xrightarrow{T_u} & V \end{array} \tag{2}$$

is commutative.

The quadratic form $q$ which will allow us to count the number of $E_{p^5}$'s of $G$ is given by

$$q(v) = v \cdot T_u(v) \qquad \text{all } v \in V. \tag{3}$$

THEOREM 3.2. *Let $G$ be a group of order $p^7$ and exponent $p$ with $Z(G) = G'$ of order $p^3$. In addition, assume that some maximal subgroup of $G$ does not contain an elementary abelian subgroup of order $p^5$.*

*Then there is a quadratic form $q$ on a 3-dimensional vector space over $GF(p)$ with the property:*

*There is one-to-one correspondence between the set of projective solutions to $q(v) = 0$ and the set of elementary abelian subgroups of order $p^5$ of $G$.*

*In particular, the number of elementary abelian subgroups of order $p^5$ of $G$ is equal to the number of points on one of the four projective varieties:*

| *point* | *line* | *double line* | *conic* |
|---|---|---|---|
| • | ⟋ | ✕ | ⬭ |
| 1 | $p + 1$ | $2p + 1$ | $p + 1$ |

*Proof.* The quadratic form $q$ is just that of (3) assigned to a maximal subgroup $A$ of $G$ which does not contain an $E_{p^5}$ (cf. Sections 3A and 3B).

We now show how the $E_{p^5}$'s of $G$ are related to nonzero solutions of the quadratic form $q(v) = 0$. If $E$ is an $E_{p^5}$ of $G$, then $|E \cap A/Z(G)| = p$; furthermore, any $a \in A \cap E - Z(G)$ is centralized by some element outside of the maximal subgroup $A$; specifically:

$$1 = [a, ub] \qquad \text{for some } b \in A,$$

whence $E = \langle a, ub, Z(G) \rangle$.

Thus when $E$ is an $E_{p^5}$, there is an element $a \in A - Z(G)$ such that

$$[a, b] = [u, a] \qquad \text{for some } b \in A \tag{4}$$

Converting the last equality to cross products and the linear mapping $T_u$ on $V$ (cf. Eqs. (1) and (2)) we get a nonzero $v \in V$ such that

$$v \times w = T_u(v) \qquad \text{for some } w \in V.$$

By the relationshop between the cross and dot products (3.1) this just says that

$$q(v) = v \cdot T_u(v) = 0 \qquad \text{for some nonzero } v \in V.$$

If $a'$ were another element of $A \cap E - Z(G)$, then the corresponding element $v'$ of $V$ would be a nonzero scalar multiple of $v$, i.e., $v$ and $v'$ both define the same projective point. Furthermore, if $E \cap A = E' \cap A$, it follows easily that $E = E'$. Thus the $E_{p^5}$'s of $G$ are in one-to-one correspondence a subset of the projective variety associated to the quadratic form $q$.

To complete the proof we must show that to each nonzero solution $v$ to $q(v) = 0$, there is an $E_{p^5}$, $E$, such that $v$ corresponds to an element of $A \cap E - Z(G)$. But this is easy. For if $v$ is a nonzero solution to $v \cdot T_u(v) = 0$ then by (3.1)

$$v \times w = T_u(v) \qquad \text{for some } w \in V.$$

Converting back to $A$, this says there is an element $a \in A - Z(G)$ such that (4) is satisfied for some element $b \in A$. Thus $E = \langle a, ub, Z(G) \rangle$ is an $E_{p^5}$ of $G$; furthermore $a \in E \cap A - Z(G)$ as needed to complete the proof of the one-to-one correspondence.

The rest of the theorem follows from the known properties of the solutions to $q(v) = 0$ where $q$ is a quadratic form on a three dimensional vector space (cf. [17, pp. 180, 181]).

C. *Groups classified by their quadratic forms*

Let $G$ be a group of order $p^7$, exponent $p$, with $Z(G) = G'$ of order $p^5$. If some maximal subgroup $A$ of $G$ does not contain an $E_{p^5}$, then (Theorem 3.2) there is assigned to $G$ a quadratic form which determines the lattice of $E_{p^5}$'s of $G$. We will use known information about quadratic forms on a three dimensional vector space over a finite field to classify the groups under discussion.

Recall that the quadratic form $q$ is given by $q(v) = v \cdot T_u(v)$, where $T_u$ is a linear mapping on a 3-dimensional vector space $V$ with basis $i, j, k$; specifically to each choice $\bar{a}_1$, $\bar{a}_2$, $\bar{a}_3$ of basis of $A/Z(G)$ there are isomorphisms $\phi, \gamma$ such that diagram (2) is commutative. If $\bar{a}_1'$, $\bar{a}_2'$, $\bar{a}_3'$ is another choice of a basis of $A/Z(G)$ then we get a commutative diagram:

$$\begin{array}{ccc} V & \xrightarrow{T_{u'}} & V \\ {\scriptstyle\phi'}\uparrow & & \uparrow{\scriptstyle\gamma'} \\ A/Z(G) & \xrightarrow{[u,\ ]} & G' \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\gamma} \\ V & \xrightarrow{T_u} & V \end{array} .$$

It follows that if $P$ is the matrix of the change of basis on $A/Z(G)$, then the corresponding change of basis on $G'$ is given by $(P^{-1})^{\mathrm{tr}} \det(P)$. Thus the matrices $M$, $M'$ of $T_u$, $T_{u'}$, respectively, are related by

$$(\det P)\, M' = PMP^{\mathrm{tr}}.$$

This is congruence up to a scalar mutiple. This multiple can be eliminated and, moreover, $M$ can be taken to be a symmetric matrix because of the following two observations:

first, if $a \in A$, then $T_a$ is represented by a skew symmetric matrix and each $3 \times 3$ skew symmetric matrix over $GF(p)$ is of this form;

second, if $u' = u^n a$, then $T_{u'} = nT_u + T_a$.

Thus, by choosing $a$ properly, $T_u$ can be represented by a symmetric matrix. Then by proper choice of the basis of $A/Z(G)$, and replacing $u$ by a power of $u$ if necessary, the matrix for $T_u$ may be replaced by any element in the equivalence class under congruence of matrices. Thus by using known results for quadratic forms on a 3 dimensional vector space over a finite field of characteristic $\neq 2$ the matrix of $T_u$ can be taken to be one of the following four diagonal matrices $(0, 1, -q)$, $(0, 0, 1)$, $(0, 1, -1)$, $(1, 1, -1)$, where $q$ is not a square modulo $p$ (cf. [15, Chap. 1]). Thus by suitable basis change and suitable choice of $u$, the mapping $T_u$ can be represented by one of the four matrices:

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -q \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix},$$

$q$ not a square mod $p$.

These lead to the point, line, double line, and conic groups, respectively (cf. Table I below).

Implicit in the classification listed in the table below is that exponent $p$ groups of class 2 are determined by their commutator relations; for a formal proof of this see [14, Section 1].

Thus, we have enough information to classify the groups of type I given in the following Table I. The information needed for type II will be given after we look at those groups which are the products of two $E_{p^5}$'s.

TABLE I

Groups $G$ of Order $p^7$, Exponent $p$, with $Z(G) = G'$ of Order $p^3$

$G = \langle u, a_1, a_2, a_3 \rangle$; $Z(G) = \langle z_1, z_2, z_3 \rangle$

I. Some maximal subgroup $A$ does not contain an $E_{p^5}$

$[a_2, a_3] = z_1$, $[a_3, a_1] = z_2$, $[a_1, a_2] = z_3$, and $[u, a_1] = 1$.

| group: | point | line | double line | conic |
|---|---|---|---|---|
| | • |  |  |  |
| number of $E_{p^5}$'s: | 1 | $p + 1$ | $2p + 1$ | $p + 1$ |
| quadratic form: | $X_2^2 - qX_3^2$ $q$ not a sq. mod $p$ | $X_3^2$ | $X_2X_3$ | $X_2^2 - X_1X_3$ |
| $[u, a_2]$: | $[a_3, a_1]$ | 1 | 1 | $[a_3, a_1]$ |
| $[u, a_3]$: | $[a_1, a_2]^{-q}$ | $[a_1, a_2]$ | $[a_3, a_1]$ | $[a_2, a_3]^{-1}$ |

II. Every maximal subgroup contains an $E_{p^5}$ (the plane group)

$[a_i, a_j] = 1$ and $[u, a_i] = z_i$, $1 \leqslant i, j \leqslant 3$.

The number of $E_{p^5}$'s in $G$ is equal to the number $(p^2 + p + 1)$ of $E_{p^5}$'s in the unique $E_{p^6}$ ($A = \langle a_1, a_2, a_3, Z(G) \rangle$) of $G$; i.e., to the number of points in the projective plane.

*Remarks* 3.3. (i) In the single line group all $E_{p^5}$'s are contained in the maximal subgroup $\langle u, a_1, a_2, Z(G) \rangle$.

(ii) The double line group is the product of any two of its $E_{p^5}$'s neither of which is the unique $E_{p^5}$, $\langle u, a_1, Z(G) \rangle$.

(iii) The conic group is the product of any two of its $E_{p^5}$'s.

D. *Products of two $E_{p^5}$'s*

The double line group and the conic group are the products of two normal $E_{p^5}$'s:

$$G = E_1E_2 \quad \text{with} \quad G' = [E_1, E_2] = E_1 \cap E_2 = Z(G); \tag{5}$$

they are distinguished by the form of the kernel of the mapping:

$$\begin{aligned} [\ ,\ ]\colon \bar{E}_1 \otimes \bar{E}_2 &\to G' \\ x_1Z \otimes x_2Z &\to [x_1, x_2]. \end{aligned} \tag{6}$$

Any group $G$ of the form (5) is determined by its commutator mapping (6). Thus by treating $\bar{E}_1 = E_1/Z(G)$ and $\bar{E}_2 = E_2/Z(G)$ as additive vector spaces, (they are 2 dimensional) there are bases $\bar{x}_i$ , $\bar{y}_i$ of $\bar{E}_1$ , $i = 1, 2$ such that either (1) $\bar{x}_1 \otimes \bar{x}_2$ generates the kernel or (2) $\bar{x}_1 \otimes \bar{x}_2 - \bar{y}_1 \otimes \bar{y}_2$ generates the kernel and the form of the kernel is independent of the choice of basis [7, p. 21].

In group theoretic terms the two $E_{p^5}$'s, $E_1$ and $E_2$ , can be written

$$E_i = \langle x_i , y_i , Z(G)\rangle, \qquad i = 1, 2,$$

where either (1) $[x_1 , x_2] = 1$ or (2) $[x_1 , x_2] = [y_1 , y_2]$. We will show that (1) corresponds to the double line group and that (2) corresponds to the conic group.

In the first case, direct calculation shows that $G$ has just the $2p + 1$ $E_{p^5}$'s:

$$\begin{gathered}\langle x_1 , x_2 y_1^{\,i}, Z(G)\rangle, \langle x_1 y_2^{\,j}, x_2 , Z(G)\rangle \; 0 \leqslant i, j \leqslant p - 1 \\ E_1 = \langle x_1 , y_1 , Z(G)\rangle, \qquad E_2 = \langle x_2 , y_2 , Z(G)\rangle.\end{gathered} \tag{7}$$

Furthermore, $\langle x_1 x_2 , y_1 , y_2 , Z(G)\rangle$ is a maximal subgroup which does not contain an $E_{p^5}$ .

Thus when the kernel of the mapping in (6) is of the form $\langle \bar{x}_1 \otimes \bar{x}_2\rangle$, the corresponding group is the double line.

When the kernel is of the second type, corresponding to the relation $[x_1 , x_2] = [y_1 , y_2]$, direct calculation shows that $G$ has just the $p + 1$ $E_{p^5}$'s:

$$\langle x_1 y_2^{\,i}, y_1 x_2^{\,i}, Z(G)\rangle, \quad i = 0,..., p - 1 \quad \text{and} \quad E_2 = \langle x_2 , y_2 , Z(G)\rangle. \tag{8}$$

Furthermore, $\langle x_1 x_2 , y_1 , y_2 , Z(G)\rangle$ is a maximal subgroup which does not contain an $E_{p^5}$ . Thus $G$ is the conic group when the kernel is of the second type.

In particular we have shown the following.

THEOREM 3.4. *Let a group $G$ be the product of two normal elementary abelian subgroups of order $p^5$; $G = E_1 E_2$ , such that*

$$[E_1 , E_2] = E_1 \cap E_2 = Z(G).$$

*Then $G$ is either the double line group or the conic group.*

E. *The Line Lemma fails for the conic group*

Let $G$ be the conic group. We want to show that the Line Lemma 1.4 fails for $G$; that is, for each maximal subgroup $M_1$ containing an $E_{p^5}$ there is

another maximal subgroup $M_2$ containing an $E_{p^5}$ such that not every maximal subgroup $M$ on the line $\overline{M_1M_2}$ has an $E_{p^5}$. In fact, we will show $M_1$ and $M_2$ are the only points on $\overline{M_1M_2}$ which contain an $E_{p^5}$.

First, notice that if $E_1$, $E_2$ are any distinct pair of $E_{p^5}$'s of the conic group $G$, then $E_1E_2 = G$ and we may choose $x_i, y_i \in E_i$, $i = 1, 2$ such that $E_i = \langle x_i, y_i, Z(G)\rangle$ and $[x_i, x_2] = [y_1, y_2]$. It will be helpful to note that by (8)

(3.5) a noncentral element $x_1^a y_1^b x_2^c y_2^d$ is an element of some $E_{p^5}$ of the conic group if and only if $\det\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] = 0$.

Any maximal subgroup $M_1 \geqslant E_1$ has the form $M_1 = \langle x_1, y_1, x_2^\alpha y_2^\beta, Z(G)\rangle$. Choose $(\gamma, \delta)$ with $\det\left[\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right] \neq 0$ and set $M_2 = \langle x_2, y_2, x_1^\gamma y_1^\delta, Z(G)\rangle$. Then $M_2$ is a maximal subgroup of $G$ containing $E_2$ and

$$M_1 \cap M_2 = \langle x_1^\gamma y_1^\delta, x_2^\alpha y_2^\beta, Z(G)\rangle.$$

It follows from (3.5) that no element of $M_1 \cap M_2 - (E_1 \cap E_2)$ is in an $E_{p^5}$ which implies that no maximal $M \geqslant M_1 \cap M_2$ except $M_1$ or $M_2$ contains an $E_{p^5}$. Thus the Line Lemma fails for the conic group.

F. *Groups where every maximal subgroup has an $E_{p^5}$*

In order to complete the classification given in Table I we need the following proposition.

PROPOSITION 3.6. *Let $G$ be a group of order $p^7$ and exponent $p$ with $Z(G) = G'$ of order $p^3$. In addition, assume that every maximal subgroup of $G$ contains an elementary abelian subgroup of order $p^5$.*

*Then $G$ has a unique elementary abelian subgroup of order $p^6$ which contains all of the elementary abelian subgroups of order $p^5$ of $G$. In particular, $G$ has just $p^2 + p + 1$ elementary abelian subgroups of order $p^5$.*

*Proof.* If each maximal subgroup of $G$ contains an $E_{p^5}$ then $G$ cannot be the product of two of its $E_{p^5}$'s (cf. Theorem 3.4). Thus $G$ has a maximal subgroup $M$ which is the product of two $E_{p^5}$'s: $M = E_1E_2$. We will first show that $M = E_1E_2$ contains all of the $E_{p^5}$'s of $G$ and then we will show $M$ abelian.

Suppose $E_3$ is an $E_{p^5}$ not contained in $M = E_1E_2$. Then by order considerations $G = E_1E_2E_3$ and $Z(G) = E_1 \cap E_2 \cap E_3$, whence

$$E_3 \geqslant E_3 \cap (E_1E_2) \geqslant (E_3 \cap E_1) \cdot (E_3 \cap E_2).$$

The latter group has order $p^2$ over $Z(G)$, hence

$$E_3 = (E_3 \cap E_1) \cdot (E_3 \cap E_2) \leqslant E_1E_2$$

contradicting the assumption that $E_3 \nleqslant E_1E_2$. Hence all the $E_{p^5}$'s of $G$ are contained in the maximal subgroup $M = E_1E_2$.

In order to show that $M = E_1E_2$ is abelian it suffices to show that each of its maximal subgroups $L$ is abelian. Such an $L$ is the intersection of $M$ and a maximal subgroup $M_1$ of $G$. Because each maximal subgroup of $G$ has an $E_{p^5}$ and because all $E_{p^5}$'s are in $M$, the intersection $L = M \cap M_1$ being of order $p^5$ must be an $E_{p^5}$ and so be abelian. Thus $M = E_1E_2$ is abelian as claimed.

## 4. Counting Elementary Abelian Subgroups of Rank 5

In this section we count, modulo $p$, the number of elementary abelian subgroups of order $p^5$, $p \neq 2$, of a $p$-group. We use the full Flow Chart 1.8 and the counting and existence results of Theorem 3.2. In contrast to counting $E_{p^5}$'s for $k \leqslant 4$, when $k = 5$ we must do the counting in the product of two normal $E_{p^5}$'s by a method other than the Line Lemma 1.4 as the Line Lemma does not hold for the conic group, cf. 3.E. Moreover, information about just two normal $E_{p^5}$'s is not sufficient to complete the proof—we must examine the product of three normal $E_{p^5}$'s.

The normality result of the following theorem is Theorem B of [16].

Main Theorem 4.1. *Let $G$ be a finite $p$-group, $p \neq 2$, containing an elementary abelian subgroup of order $p^k$, $k \leqslant 5$.*

*Then the number of elementary abelian subgroups of $G$ of order $p^k$, $k \leqslant 5$, is congruent to one modulo $p$.*

*Further, if a normal subgroup $N$ of $G$ contains an elementary abelian subgroup of order $p^k$, $k \leqslant 5$, then $N$ contains one which is normal in $G$.*

*Proof.* The proof for $k \leqslant 4$ is given in Theorem 2.2. Thus we restrict our attention to $E_{p^5}$'s.

We may assume, by induction, that the theorem has been verified for groups of order less than $|G|$, in particular, for the maximal subgroups $M$ of $G$. Let $\mathscr{C}$ be the class of all elementary abelian subgroups of $G$ of order $p^5$.

As was explained in the Application 1.7 we may restrict ourselves to the case where $G$ has at least two normal $E_{p^5}$'s. In terms of the Flow Chart 1.8 we may assume that there are two normal $E_{p^5}$'s, $E_1$, and $E_2$, whose commutator $[E_1, E_2]$ has order $p^3$. For otherwise (as in the proof of 2.2) Theorem 2.1 would imply the existence of a local origin or would say that all normal pairs of $E_{p^5}$'s would support good lines, which would complete the proof in this case.

If there were no normal $E$ in $\mathscr{C}$ not in $E_1E_2$, then $n(G) \equiv n(E_1E_2) \equiv 1 \bmod p$

by Proposition (0.1 v) and Theorem 3.2. Furthermore, if each such $E$ supported good lines with one or the other of $E_1$, $E_2$, then by Method 1.6 iii, any maximal subgroup $M_0 \geqslant E_1E_2$ would be an origin for the Line Lemma. Hence, by 2.1, we may assume there is a normal subgroup $E_3 \in \mathscr{C}$ with $E_3 \not\leqslant E_1E_2$ and with both $[E_1, E_3] = Z(E_1E_2)$ and $[E_2, E_3] = Z(E_2E_3)$ of order $p^3$.

We will now show that the product $E_1E_2E_3$ is a local origin where $E_i$ are normal elements of $\mathscr{C}$, $E_3 \not\leqslant E_1E_2$ and $[E_i, E_j] = E_i \cap E_j = Z(E_iE_j)$ has order $p^3$ for $i \neq j$.

Depending on the order of the triple intersection $D = E_1 \cap E_2 \cap E_3$, we will either use Theorem 3.2 to conclude that each maximal subgroup of $P = E_1E_2E_2$ contains an $E_{p^5}$ or exhibit an $E_{p^5}$ contained in $P' \leqslant \Phi(G)$. In both cases this says $E_1E_2E_3$ is a local origin. So an application of the Line Lemma will complete the proof.

If $D$ has order $p^3$ then $P$ is a class 2 group of exponent $p$ and order $\geqslant p^8$ with $Z(P) = P' = D$ of order $p^3$. Thus each maximal subgroup $L$ of $P$ contains an $E_{p^5}$ (cf. Theorem 3.2 and the proof of 2.1 if $|L'| \leqslant p^2$).

If $D$ has order $\leqslant p^2$, then $(E_1 \cap E_2) \cdot (E_1 \cap E_3) \cdot (E_2 \cap E_3)$ is local origin since it is an abelian subgroup of $P' \leqslant \Phi(G)$ of order at least $p^5$. This completes the proof of counting modulo $p$.

The normality results then follow from Proposition 0.1 iv.

## 5. Counting Abelian Subgroups of $p$-Groups

In this section we count, modulo $p$, the number of abelian subgroups of order $p^k$, for $k \leqslant 5$, of a $p$-group, $p \neq 2$. We again use the full Flow Chart 1.8. To do this we develop analogues to Theorem 2.1 giving criteria for finding local origins and for the support of good lines. As in the elementary abelian case, Theorem 4.1, we use the decision procedures of the Flow Chart 1.8 to reduce the problem to showing that a certain product of three abelian subgroups of order $p^5$ is a local origin. But this product is isoclinic [10] to the corresponding product $P$ of three $E_{p^5}$'s appearing in the proof of Theorem 4.1. As isoclinic groups have the same number of maximal abelian subgroups, this gives enough information to complete the proof.

Theorem [6] 5.1. *Let $G$ be a class 2 $p$-group with cyclic commutator group of order $p^\alpha$. Then*

(i) *$G$ is the central product of groups $H$ with*

$$H/Z(H) \simeq Z_{p^\beta} \times Z_{p^\beta} \qquad \text{for} \quad 1 \leqslant \beta \leqslant \alpha.$$

(ii) *An abelian subgroup $A$ of $G$ is maximal abelian if and only if*

$$Z(G) \leqslant A \quad \text{and} \quad |A: Z(G)| = |G: Z(G)|^{1/2}.$$

The following corollary is the analogue to Theorem 2.1 when $G'$ is cylcic.

COROLLARY 5.2. *Let $G$ be a class 2 $p$-group, $p \neq 2$ such that $G'$ is cyclic, and let $G' \leqslant N \leqslant Z(G)$, where $|G: N| = p^n$.*
*Then $G$ contains an abelian subgroup $A \geqslant N$ with $|A : N| = p^{[(n+1)/2]}$.*

We need the same conclusion for $G'$ abelian of rank 2.

THEOREM 5.3. *Let $G$ be a $p$-group of class 2, $p \neq 2$, such that $G'$ is an abelian subgroup of rank 2, and let $G' \leqslant N \leqslant Z(G)$, where $|G: N| = p^n$.*
*Then $G$ contains an abelian subgroup $A \geqslant N$ with $|A: N| = p^{[(n+1)/2]}$.*

*Proof.* We begin by considering three special cases.

First, if $G/N$ has exponent $p$, then $G'$ has exponent $p$. The Theorem reduces to Alperin's Theorem on two alternating forms [1, Theorem 3] (cf. proof of 2.1).

Second, if $G/N$ is isomorphic to the direct product of $k$ cyclic groups of order $p^{2i}$ for some integer $i$, then $A = \mathcal{O}^i(G) \cdot N$ has the desired property.

Third, if $G/N$ is isomorphic to the direct product of $k$ cyclic groups of order $p^{2i+1}$ for some integer $i \geqslant 1$, then let $D = \mathcal{O}^{i+1}(G) \cdot N$ and $C = \mathcal{O}^i(G) \cdot N$. We note that $C' \leqslant D \leqslant Z(C) \leqslant C$ and $C/D$ is vector space of dimension $k$. Hence we see (by the first case above, that $C$ contains an abelian subgroup $A \geqslant D$ with $|A/D| = p^{[(k+1)/2]}$. Hence

$$|A: N| = |A: D|\,|D: N| = p^{[(k+1)/2]+ik};$$

because $[(k+1)/2] + ik = [((2i+1)\,k+1)/2]$, the group A has the desired property.

Now in the general case we write

$$G/N = P_1/N \times \cdots \times P_m/N,$$

where each $P_\alpha/N$ is isomorphic to the direct product of $k_\alpha$ cyclic groups of order $p^\alpha$. By the above special cases we can find abelian subgroups $A_\alpha$ so that $N \leqslant A_\alpha \leqslant P_\alpha$ and $|A_\alpha : N| = p^{[(n_\alpha+1)/2]}$ where $p^{n_\alpha} = |P_\alpha : N|$. Furthermore, if $\alpha < \beta$, then

$$\begin{aligned}[A_\alpha, A_\beta] &\leqslant [\mathcal{O}^{[\alpha/2]}(P_\alpha), \mathcal{O}^{[\beta/2]}(P_\beta)] \\ &\leqslant [P_\alpha, \mathcal{O}^{[\alpha/2]+[\beta/2]}(P_\beta)] \\ &\leqslant [P_\alpha, Z(G)] = 1.\end{aligned}$$

So by choosing $A = A_1 \times A_2 \times \cdots \times A_m$ the result follows.

The following Theorem is the abelian subgroup analog to Theorem 2.1.

THEOREM 5.4. *Let $H = A_1A_2$ be the product of two normal abelian subgroups $A_1 \neq A_2$, each of order $p^k$, $p \neq 2$, such that either $H'$ has rank at most 2 or $Z(H)$ has index at most $p^2$ in $H$.*

*Then either $H$ contains an abelian subgroup of order $p^{k+1}$ or each maximal subgroup $L \geqslant A_1 \cap A_2$ of $H$ contains an abelian subgroup of order $p^k$.*

*The first conclusion implies that the product $A_1A_2$ is a local origin and both say that the pair $A_1$, $A_2$ supports good lines for the class $\mathfrak{C}$ of all abelian subgroups of order $p^k$ of any $p$-group $G$ containing both $A_1$ and $A_2$.*

*Proof.* $H$ has class at most 2 and $Z(H) \geqslant A_1 \cap A_2$, because $A_1$ and $A_2$ are abelian normal subgroups of $H$. If $Z(H) > A_1 \cap A_2$, then either $A_1Z(H)$ or $A_2Z(H)$ is abelian of order at least $p^{k+1}$.

If $Z(H) = A_1 \cap A_2$ has order $p^c$, then $|H| = p^{2k-c}$ and any maximal subgroups $L \geqslant A_1 \cap A_2$ of $H$ satisfies $|L: Z(H)| = p^{2(k-c)-1}$. Thus $L$ contains an abelian subgroup $A \geqslant Z(H)$ with $|A: Z(H)| = p^{k-c}$ (by 5.2, 5.3 or by inspection when $Z(H)$ has index $p^2$ in $H$ in which case $c = k - 1$). Since $|A| = p^k$, this completes the proof.

THEOREM 5.5. *Let $G$ be a finite $p$-group, $p \neq 2$, containing an abelian subgroup of order $p^k$, $k \leqslant 5$.*

*Then the number of abelian subgroups of order $p^k$ of $G$ is congruent to 1 modulo $p$.*

*Further, if a normal subgroup $N$ of $G$ contains an abelian subgroup of order $p^k$, then $N$ contains one which is normal in $G$.*

*Proof.* We again use the full Flow Chart 1.8 as in the proof of the Main Theorem 4.1. Theorem 5.4 (the analogue of 2.1) tells us that if a normal pair $A_1$, $A_2$ of abelian subgroups of order $p^k$, $k \leqslant 5$ does not support good lines then $A_1$, $A_2$ are of order $p^5$ and $[A_1, A_2] = A_1 \cap A_2 = Z(A_1A_2)$ is of order $p^3$. This implies that the product $A_1A_2$ is isoclinic to a product $E_1E_2$ of normal $E_{p^5}$'s with $[E_1, E_2] = E_1 \cap E_2 = Z(E_1E_2)$ of order $p^3$. For the central quotient of $A_1A_2$ is the direct product of the two groups $A_i/A_1 \cap A_2$, $i = 1, 2$ of order $p^2$. Furthermore, these two groups are either both cyclic of order $p^2$ or elementary abelian of order $p^2$ because of the fact that the two highest invariant factors must be equal for the central quotient of a class two group [8, p. 13]. The cyclic $p^2$ case is ruled out as $A_1A_2$ would then have a commutator group of order $p^2$ rather than the given order $p^3$. Thus the only possibility is that $[A_1, A_2]$ is elementary abelian as needed for the stated isoclinism.

The product $A_1A_2$ being isoclinic to the product $E_1E_2$ of a pair of normal $E_{p^5}$'s with $|[E_1, E_2]| = p^3$ implies that both $A_1A_2$ and $E_1E_2$ have the same

number of abelian subgroups of order $p^5$. This number is $\equiv 1 \bmod p$ by Theorem 3.2 ($E_1E_2$ has exponent $p$, as $p \neq 2$).

Just as in the proof of 4.1, the Flow Chart 1.8 via 5.4 leads us to a product $A_1A_2A_3$ of three normal abelian subgroups of order $p^5$ with $[A_i, A_j] = A_1 \cap A_j = Z(A_iA_j)$ of order $p^3$ for $i \neq j$.

If the triple intersection $A_1 \cap A_2 \cap A_3$ has order $p^3$, then $A_1A_2A_3$ is isoclinic to the group $P = E_1E_2E_3$ dealt with the proof of 4.1. Hence by isoclinism, $A_1A_2A_3$ is a local origin.

If $A_1 \cap A_2 \cap A_3$ has order $\leqslant p^2$, then, as in 4.1, the group $(A_1 \cap A_2) \cdot (A_1 \cap A_3) \cdot (A_2 \cap A_3)$ is abelian of order $\geqslant p^5$ contained in $(A_1A_2A_3)' \leqslant \Phi(G)$. This completes the proof of counting modulo $p$.

The normality results then follow from Proposition 0.1 iv.

Similarly one proves:

THEOREM 5.6. *Let $G$ be a $p$-group, $p \neq 2$ for which all abelian subgroups of $G'$ have rank at most 2. Suppose $G$ has an abelian subgroup of order $p^k$.*

*Then the number of abelian subgroups of order $p^k$ of $G$ is congruent to 1 modulo $p$.*

## 6. COUNTING ABELIAN SUBGROUPS OF INDEX $p^2$

In this section we count, modulo $p$, the number of abelian subgroups of index $p^2$ in a $p$-group $G$, $p \neq 2$. It is surprising to note that instead of the almost ubiquitous result $n(G) \equiv 1 \bmod p$, we run into groups with exactly two abelian subgroups of index $p^2$. Thse groups are all isoclinic to a group $\mathcal{O}$ which is the product of two normal $E_{p^6}$'s and these are the only $E_{p^6}$'s in $\mathcal{O}$. For a more detailed study of such examples see [14, Section 3].

Our counting result gives, as an immediate corollary, Alperin's result [1, Theorem 4] that a $p$-group, $p \neq 2$, which contains an abelian subgroup of index $p^3$ contains a normal abelian subgroup of index $p^3$.

THEOREM 6.1. *Let $G$ be a $p$-group.*

(i) *Let $G$ contain an abelian subgroup of index $p$. Then the number of abelian subgroups of index $p$ is congruent to one modulo $p$.*

(ii) *Let $G$ contain an abelian subgroup of index $p^2$, $p \neq 2$.*

*Then either*

(a) *the number of abelian subgroups of index $p^2$ of $G$ is congruent to 1 modulo $p$, or*

(b) *$G$ contains exactly two abelian subgroups of index $p^2$.*

*In the latter case, $G$ is isoclinic to the class 2 group of order $p^8$, exponent $p$, with generators $x_1, y_1, x_2, y_2$ with the additional relations $[x_i, y_i] = 1$, $i = 1, 2$.*

*Proof.* The index $p$ case is well known; when $G$ is non-abelian the number is either 1 or $p + 1$. In terms of the Line Lemma 1.4 any abelian subgroup of index $p$ in $G$ is an origin.

We now consider the index $p^2$ case. Let $\mathscr{C}$ be the class of abelian subgroups of index $p^2$ in $G$. By the above remarks we have that $n(M) = 0$ or $n(M) \equiv 1 \bmod p$ for each maximal subgroup $M$ of $G$.

As before (cf. Application 1.7) we may assume that $\mathscr{C}$ contains at least two normal elements $A_1, A_2$ of $\mathscr{C}$. If their product $A_1A_2$ is a maximal subgroup of $G$, then every subgroup $L$ with $A_1 \cap A_2 < L < A_1A_2$ is abelian of index $p^2$ in $G$. So such a pair supports good lines. Thus we are done, by the Line Lemma, unless there is a normal pair $A_1, A_2$ of elements of $\mathscr{C}$ with $G = A_1A_2$.

Let $A_1, A_2$ be a normal pair of elements of $\mathscr{C}$ with $G = A_1A_2$. We show that, with one exception, $G$ is isoclinic to the product of two normal abelian subgroups of order $\leqslant p^5$, allowing us to use Theorem 5.5. Since $G = A_1A_2$, it follows that $Z(G) \geqslant A_1 \cap A_2$ has index $\leqslant p^4$ in $G$ and

$$| A_iZ(G)/Z(G)| \leqslant | A_i/A_1 \cap A_2 | = p^2, \qquad 1 = 1, 2,$$

so that $G' = [A_1, A_2]$ has order $\leqslant p^4$.

Thus except in the case where $G' = [A_1, A_2]$ has order $p^4$, $G$ is isoclinic to a group $H$ of order dividing $p^7$ whose abelian subgroups of index $p^2$ are just the abelian subgroups of order $p^k$ of $H$ for a suitable $k$, $k \leqslant 5$. Thus by isoclinism and Theorem 5.5 we see that the number of abelian subgroups of index $p^2$ of $G$ is congruent to 1 modulo $p$ as long as $| G' | \leqslant p^3$.

In the remaining case, $| G' | = p^4$, the number is exactly two. For then $G$ is isoclinic to the class 2 group $\mathscr{A}$ of order $p^8$, exponent $p$, with generators $x_1, y_1, x_2, y_2$ subject to the additional relations: $[x_i, y_i] = 1$, $i = 1, 2$. Such groups have only two abelian subgroups of order $p^6$ (index $p^2$) (cf. [13, p. 349] and Section 3 of [14]). This completes the proof of the count modulo $p$.

The first part of the following was first proven by Konvisser [16, Theorem A], the second by Alperin [1, Theorem 4].

THEOREM 6.2. *Let $N$ be a normal subgroup of a $p$-group $G$, $p \neq 2$. Suppose there is an abelian subgroup of index $p^2$ in $N$.*

*Then $N$ contains an abelian subgroup of index $p^2$ in $N$ which is normal in $G$.*

*In particular, if $G$ contains an abelian subgroup of index $p^3$, $p \neq 2$, then it has a normal abelian subgroup of index $p^3$.*

*Proof.* Follows directly from the counting result of 6.1 and Proposition 0.1 iv.

## REFERENCES


1. J. L. ALPERIN, Large Abelian subgroups of $p$-groups, *Trans. Amer. Math. Soc.* **117** (1965), 10–20.
2. J. G. BERKOVIC, Subgroups, normal subgroups and epimorphic images of a $p$-group of finite order, *Sov. Math. Dokl.* **10** (1969), 878–881.
3. J. G. BERKOVIC, Subgroup and normal structure of a finite $p$-group, *Sov. Math. Dokl.* **12** (1971), 71–75.
4. J. G. BERKOVIC, On a nonregular $p$-group, *Siberian Math. J.* **12** (1971), 654–657.
5. W. FEIT AND J. G. THOMPSON, Solvability of groups of odd order, *Pacific J. Math.* **13** (1963), 755–1029.
6. R. GILMAN AND K. JOSEPH, unpublished.
7. W. H. GREUB, "Multilinear Algebra," Springer–Verlag, Berlin and New York, 1967.
8. M. HALL, JR. AND J. K. SENIOR, "The groups of order $2^n (n \leqslant 6)$," Macmillan, New York, 1964.
9. P. HALL, A contribution to the theory of groups of a prime power order, *Proc. London Math. Soc.* **36** (1932), 29–95.
10. P. HALL, The classification of prime-power groups, *J. Reine Angew. Math.* **182** (1940), 130–141.
11. HERMAN HEINEKEN, Vektorräume mit mehreren antisymmetrischen Bilinearformen, *Arch. Math. (Basel)* **18** (1967), 449–455.
12. CHARLES HOBBY, Abelian subgroups of $p$-groups, *Pacific J. Math.* **12** (1962), 1343–1345.
13. B. HUPPERT, "Endliche Gruppen. I," Springer-Verlag, Berlin and New York, 1967.
14. D. JONAH AND M. KONVISSER, Abelian subgroups of $p$-groups, an algebraic approach, *J. Algebra*, to appear.
15. IRVING KAPLANSKY, "Linear Algebra and Geometry," Allyn and Bacon, Boston, 1969.
16. M. KONVISSER, Embedding of abelian subgroups in $p$-groups, *Trans. Amer. Math. Soc.* **153** (1971), 469–481.
17. A. SEIDENBERG, "Projective Geometry," Van Nostrand, Princeton, 1962.